Specimen Question **Annexure-XXXVIII**

DO NOT OPEN THE SEAL UNTIL YOU ARE TOLD TO DO SO

QP-FSL-2024 **Question Booklet No.**

CYBER FORENSIC

PAPER—III

Test Booklet Series

A

Time Allowed : 1 Hour 30 Minutes **Maximum Marks : 150**

INSTRUCTIONS FOR CANDIDATES

1. Immediately after the commencement of the examination, you should check that this Test Booklet ***does not*** have any unprinted or torn or missing pages or questions etc. If so, get it replaced by a complete Test Booklet.

2. Write your Roll Number on the Test Booklet in the Box provided alongside.

3. This Test Booklet contains **150** questions. Each question comprises of four responses (answers) within as (A), (B), (C) and (D). You should select the response which you feel is the most ***correct*** and mark it on the OMR Answer Sheet.

4. You have to mark all your responses **ONLY** on the separate **OMR Answer Sheet** provided. Also read the directions in the **OMR Answer Sheet**. Fill in all the entries in the OMR Answer Sheet ***correctly***. **DO NOT WRITE/MARK ANYTHING EXCEPT IN THE SPACE PROVIDED FOR IT,** failing which your OMR Answer Sheet ***shall not*** be evaluated.

5. **Count** the number of **questions attempted** carefully and write it down in the space provided **in the OMR Answer Sheet**.

6. After you have completed filling in all your responses on the **OMR Answer Sheet** and the examination has concluded, **you should hand over** to the Invigilator **only the OMR Answer Sheet (in original)**. **You are permitted to take away 2nd Copy of the OMR Answer Sheet and Test Booklet**.

7. Each question carries 1 mark.

8. Candidature would be cancelled in case of non-compliance with any of these instructions.

9. **Penalty for wrong answers :**

THERE WILL BE PENALTY FOR WRONG ANSWERS MARKED BY A CANDIDATE IN THE OBJECTIVE TYPE QUESTION PAPERS.

(i) There are four alternatives for the answer to every question. For each question for which a wrong answer has been given by the candidate, 0·5 mark of the marks assigned to that question will be deducted as penalty.

(ii) If a candidate gives more than one answer, it will be treated as a **wrong answer** even if one of the given answers happens to be correct and there will be same penalty as above to that question.

(iii) If a question is left blank, i.e., no answer is given by the candidate, there will be no penalty for that question.

10. **"Mobile phones, calculators, IT gadgets, smart watch and any other electronic devices such as Bluetooth etc. are not allowed inside the premises where the examination is being conducted. Any infringements of these instructions shall entail disciplinary action including ban from future examinations."**

DO NOT OPEN THE SEAL UNTIL YOU ARE TOLD TO DO SO

1. Which of the following ***does not*** constitute a cyber crime?

(A) Refusal of service

(B) Man in the middle

(C) Phishing

(D) AES

2. Which of the following is a hacking technique in which cyber criminals create fictitious web pages or domains to deceive or obtain more traffic?

(A) Pharming

(B) Mimicking

(C) Spamming

(D) Website duplication

3. _____ are programmes or procedures that enable hackers to maintain control of a computer system.

(A) Exploits

(B) Antiviruses

(C) Firewall by-passers

(D) Worms

4. What is the primary purpose of hashing in digital forensics?

(A) To encrypt data

(B) To identify duplicates

(C) To ensure data integrity

(D) To analyze metadata

5. Which of the following tools is commonly used for forensic imaging of storage devices?

(A) Autopsy

(B) FTK Imager

(C) Wireshark

(D) Nmap

6. What is the purpose of a forensic triage?

(A) To prioritize the analysis of evidence based on its relevance

(B) To collect all data from a system

(C) To conduct a detailed analysis of all files

(D) To automate the forensic investigation process

7. What is the primary purpose of using write-blockers during forensic acquisition?

(A) To copy data faster

(B) To prevent modification of the original evidence

(C) To encrypt the evidence for security

(D) To format the storage device

8. Which file format is most commonly used for storing forensic disk images?

(A) .exe

(B) .iso

(C) .dd

(D) .jpg

9. Which forensic tool is primarily used to analyze network traffic?

(A) EnCase

(B) Wireshark

(C) FTK

(D) Burp Suite

10. What does the term 'slack space' refer to in digital forensic?

(A) Unused space on a hard drive

(B) Space between files on a hard drive

(C) Unused space in disk cluster that may contain remnants of deleted files

(D) Space used by temporary files

11. Which Windows directory contains the event log files that store security and system events?

(A) C:\Windows\System32\config

(B) C:\Windows\Temp

(C) C:\Users\Public

(D) C:\ProgramFiles

12. Which of the following file systems is typically used in Windows environments and is relevant for forensic analysis?

(A) NTFS

(B) HFS+

(C) EXT4

(D) FAT32

13. Which Windows file system feature can forensic investigators use to recover deleted files?

(A) File Allocation Table (FAT)

(B) Alternate Data Streams (ADS)

(C) Shadow Copies

(D) Disk Quotas

14. The protocol commonly used for secure data transmission over the internet is

(A) HTTP

(B) HTTPS

(C) FTP

(D) SMTP

15. Which Amendment to the IT Act introduced provisions related to the punishment for cyberterrorism and cyberattacks on critical infrastructure?

(A) Amendment Act of 2005

(B) Amendment Act of 2006

(C) Amendment Act of 2008

(D) Amendment Act of 2010

16. Which of the following is a key artefact commonly analyzed in Windows forensic investigations?

(A) /var/log/messages

(B) Windows Registry

(C) Swap partition

(D) /etc/passwd

17. Which of the following do cyber attackers commonly target for fetching IP address of a target or victim user?

(A) IP tracker

(B) e-mails

(C) Websites

(D) Web pages

18. Which of the following is a key indicator that a system may have been compromised by malware?

(A) The system clock runs faster than normal

(B) Unexplained increase in network traffic

(C) Frequent system reboots

(D) Missing operating system updates

19. Which of the following is an example of a tool that is commonly used for malware reverse engineering?

(A) IDA Pro

(B) Nessus

(C) Metasploit

(D) Burp Suite

20. What is the primary advantage of using sandboxing in malware analysis?

(A) It accelerates the malware analysis process

(B) It isolates the malware, preventing it from harming the system

(C) It automatically removes malware from the system

(D) It prevents malware from being identified

21. Which registry key would an investigator look at to find recently accessed files by a user?

(A) HKEY_LOCAL_MACHINE\SOFTWARE

(B) HKEY_CURRENT_USER\Software\Microsoft\Windows\Recent

(C) HKEY_USERS\Default

(D) HKEY_CLASSES_ROOT\System

22. Which tool is commonly used to extract and analyze email headers during a forensic investigation?

(A) FTK Imager

(B) X1 Social Discovery

(C) MailXaminer

(D) EnCase

23. Which of the following files stores the information about user accounts and passwords on a Linux system?

(A) /etc/passwd

(B) /etc/shadow

(C) /var/log/auth.log

(D) /etc/group

24. Which log file in a MacOSX system tracks system events such as shutdowns, startups and hardware events?

(A) /var/log/system.log

(B) /private/var/log/install.log

(C) /priate/var/log/asl/

(D) /private/var/log/cron

25. Which of the following is a major difference between Linux and MacOSX in terms of file system structure?

(A) MacOSX uses a journaled HFS+ file system, while Linux typically uses ext3/ext4

(B) MacOSX has no file system, while Linux uses ext4

(C) MacOSX and Linux use the same file system, ext4

(D) Linux uses NTFS, while MacOSX uses HFS+

26. Which command in Linux is primarily used for creating a file system on a disk partition or storage device?

(A) dd

(B) mkfs

(C) fdisk

(D) Is

27. Which of the following forensic tasks can be accomplished using the dd command?

(A) Cloning a hard drive

(B) Recovering deleted files

(C) Analyzing file metadata

(D) Encrypting disk data

28. What does the unmount command do in Linux-based systems?

(A) It mounts a file system

(B) It unmounts a file system safely

(C) It displays file system usage statistics

(D) It formats a storage device

29. Which of the following is a valid forensic practice when using the dmesg command to investigate a system for suspicious activity?

(A) Look for messages related to disk errors or device mounting/unmounting

(B) Check for recent logins from unauthorized users

(C) Use dmesg to read the contents of encrypted files

(D) Use dmesg to clear old system message

30. What does the following command do in a Linux system : umount/dev/sdb1?

(A) Mounts the disk partition/dev/sdb1

(B) Displays information about the partition/dev/sdb1

(C) Safely removes the partition/dev/sdb1 from the system

(D) Creates a new file system on/dev/sdb1

31. Which MacOS tool can be used to retrieve the system's file access times, creation dates and other metadata from files for forensic investigation?

(A) stat

(B) Is-I

(C) fstat

(D) diskutil

32. Which MacOS command-line tool provides information about active processes running on the system and can be helpful in identifying suspicious malicious activity?

(A) top

(B) ps

(C) netstat

(D) sudo

33. Which of the following is a forensic artefact that can be analyzed on MacOS systems to investigate user activity or app usage?

(A) bash_history file

(B) SystemPreferences plist files

(C) ~/Library/Preferences

(D) All of the above

34. Which option with the find command in MacOS is used to search for files modified in the last 7 days?

(A) -mtime-7

(B) -ctime+7

(C) -atime7

(D) -size7

35. How can the find command be used to locate all files with a.log extension in a directory?

(A) find.-name“∗.log”

(B) find.-typefile“∗.log”

(C) find.-log“∗.log”

(D) find.-file“∗.log”

36. What is the impact of DNS spoofing?

(A) Disrupting a website's functionality

(B) Redirecting users to malicious websites

(C) Encrypting DNS queries

(D) Slowing down internet connections

37. What is the primary purpose of forensic analysis of cloud-connected IoT devices?

(A) To identify user interaction patterns

(B) To extract device usage history

(C) To collect evidence stored on the cloud

(D) All of the above

38. Which of the following is ***not*** a component of cloud computing?

(A) Network

(B) Storage

(C) Internet of Things (IoT)

(D) Computing resources

39. In IoT, what is the function of the perception layer?

(A) To process and analyze data

(B) To detect and collect physical information

(C) To manage communication between devices

(D) To store data in the cloud

40. In IoT forensics, which protocol is often analyzed to identify device communication patterns?

(A) TCP

(B) MQTT

(C) FTP

(D) SNMP

41. What is the function of a forensic hypervisor in a virtualized environment?

(A) To enhance server performance

(B) To isolate virtual machines for forensic analysis

(C) To encrypt forensic evidence

(D) To monitor network traffic

42. Which of the following tools is commonly used for forensic analysis in virtualized environments?

(A) FTK Imager

(B) Volatility

(C) EnCase

(D) All of the above

43. Which of the following is a modern form of toll fraud that affects Voice over IP (VoIP) systems?

(A) VoIP toll fraud

(B) SMS phishing

(C) Web defacement

(D) Email spoofing

44. Which storage format in digital forensics allows for data compression while maintaining the integrity of the evidence?

(A) ZIP

(B) E01

(C) TAR

(D) MP3

45. What is the process of 'data carving' in digital forensics?

(A) Protecting encrypted data

(B) Recovering deleted files from unallocated space

(C) Altering corrupted files for forensic use

(D) Securing digital data with strong passwords

46. Under the Bankers' Book Evidence Act, 1891, what does the term 'bankers' books' include?

(A) Only printed ledgers

(B) Only physical documents

(C) Ledgers, day-books and electronic records

(D) Confidential agreements

47. Which Section in the Indian Evidence Act provides for the admissibility of information derived from electronic records stored in mobile phones or computers?

(A) Section 17

(B) Section 3

(C) Section 65B

(D) Section 67

48. Which framework is recommended for performing cloud forensic analysis?

(A) NIST Cloud Computing Forensic Framework

(B) ISO 9001 Framework

(C) GDPR Compliance Framework

(D) OWASP IoT Security Framework

49. What is a virtual disk image and why is it important in cloud forensics?

(A) A snapshot of the cloud service's terms of use

(B) A copy of a virtual machine's disk used for forensic analysis

(C) A compressed version of server logs

(D) A backup of user credentials stored in the cloud

50. Which of the following is a key organizational challenge in cloud forensics?

(A) Lack of encryption standards

(B) Inconsistent Service Level Agreements (SLAs)

(C) Absence of virtual machines

(D) High cost of cloud storage

51. Which type of network topology connects all devices to a single central point?

(A) Bus topology

(B) Star topology

(C) Ring topology

(D) Mesh topology

52. What is the main purpose of a firewall in networking?

(A) To increase bandwidth

(B) To block unauthorized access while allowing legitimate traffic

(C) To encrypt data packets

(D) To connect multiple networks

53. Which tool was famously used in the early days of phone phreaking?

(A) Blue box

(B) Red box

(C) Wiretap device

(D) Keylogger

54. Which protocol is used for error reporting and diagnostics in the Internet Layer of TCP/IP?

(A) ARP

(B) ICMP

(C) SMTP

(D) HTTP

55. Which protocol is used to transfer files between hosts?

(A) FTP

(B) SNMP

(C) SSH

(D) DHCP

56. How many bits are there in an IPv4 address?

(A) 16 bits

(B) 32 bits

(C) 64 bits

(D) 128 bits

57. Which of the following is an example of a valid private IP address?

(A) 172.16.5.4

(B) 8.8.8.8

(C) 192.0.2.1

(D) 1.1.1.1

58. Which IP class is used for multicast addressing?

(A) Class A

(B) Class B

(C) Class D

(D) Class E

59. What is the default subnet mask for a Class B IP address?

(A) 255.255.0.0

(B) 255.0.0.0

(C) 255.255.255.0

(D) 255.255.255.255

60. Which type of NAT maps one private IP address to one public IP address?

(A) Dynamic NAT

(B) Static NAT

(C) Port Address Translation (PAT)

(D) Bidirectional NAT

61. Which network topology connects devices in closed-loop?

(A) Star

(B) Bus

(C) Ring

(D) Mesh

62. In which topology does data travel in both directions?

(A) Ring

(B) Star

(C) Mesh

(D) Full-Duplex

63. Which network type typically connects multiple LANs within a city?

(A) LAN

(B) MAN

(C) WAN

(D) PAN

64. Which protocol is typically used to transfer data across WANs?

(A) TCP/IP

(B) Bluetooth

(C) Zigbee

(D) Ethernet

65. Which authority is responsible for securing and protecting critical information infrastructure in India under Section 70B of the IT Act?

(A) Cyber Appellate Tribunal (CAT)

(B) National Cyber Security Coordinator (NCSC)

(C) National Critical Information Infrastructure Protection Centre (NCIIPC)

(D) Ministry of Electronics and Information Technology (MEITY)

66. What is the best way to prevent routing table poisoning?

(A) Use static routing tables

(B) Enable weak encryption

(C) Disable firewalls

(D) Avoid VPNs

67. How does web jacking typically occur?

(A) By exploiting DNS vulnerabilities

(B) By embedding malicious code into a website

(C) By physically stealing a server

(D) By taking over a website's domain or hosting

68. Which is the first phase of hacking?

(A) Gaining access

(B) Reconnaissance

(C) Exploitation

(D) Maintaining access

69. What is the purpose of the 'Gaining Access' phase in hacking?

(A) To scan for open ports

(B) To compromise the system using exploits

(C) To maintain long-term control system

(D) To erase logs of the attack

70. Which of the following is a passive attack on a wireless network?

(A) Deauthentication attack

(B) Jamming attack

(C) Packet sniffing

(D) ARP poisoning

71. What is the primary goal of the reconnaissance phase in hacking?

(A) Identifying weaknesses in the largest system

(B) Gaining unauthorized access to the system

(C) Encrypting the target's data

(D) Defeating antivirus software

72. Which tool is commonly used for active reconnaissance?

(A) WHOIS

(B) Nmap

(C) Google Search

(D) Social Media

73. Which of the following is ***not*** a characteristic of a passive attack?

(A) Monitoring network traffic

(B) Sniffing data from communication channels

(C) Modifying transmitted data

(D) Gathering intelligence without altering the system

74. Which tool is commonly used to crack WEP and WPA encryption in wireless networks?

(A) Metasploit

(B) Wireshark

(C) Aircrack-ng

(D) Burp Suite

75. Which mobile network generation first introduced packet-switched data?

(A) 1G

(B) 2G

(C) 3G

(D) 4G

76. In IPSec, which mode encrypts the entire IP packet?

(A) Transport Mode

(B) Tunnel Mode

(C) Hybrid Mode

(D) Authentication Mode

77. Which technology uses a combination of hardware and software to isolate networks for security purposes?

(A) VLANs

(B) VPNs

(C) Firewalls

(D) IDS

78. Which IPS detection method identifies malicious activity by comparing it against a database of known patterns?

(A) Signature-based detection

(B) Anomaly-based detection

(C) Heuristic detection

(D) Behavioral detection

79. Which type of firewall filters traffic based on rules set for IP addresses and ports?

(A) Packet Filtering Firewall

(B) Application Firewall

(C) Proxy Firewall

(D) Stateful Inspection Firewall

80. Which type of intrusion detection system is best for identifying unknown threats?

(A) Signature-based IDS

(B) Anomaly-based IDS

(C) Stateful Firewall

(D) Proxy Firewall

81. What is the primary difference between an IDS and an IPS?

(A) IDS detects intrusions, while IPS prevents them

(B) IDS encrypts data, while IPS decrypts it

(C) IDS operates at the application layer, while IPS operates at the network layer

(D) IDS is hardware-based, while IPS is software-based

82. Which protocol is commonly used to secure online payment transactions?

(A) HTTP

(B) FTP

(C) HTTPS

(D) SMTP

83. Which protocol enables secure recurring payments in online transactions?

(A) 3D Secure Protocol

(B) PCI DSS Protocol

(C) Tokenization Protocol

(D) EMV Payment Protocol

84. Which of the following is a secure network application used to monitor and filter web traffic?

(A) Web Proxy

(B) Virtual LAN

(C) Web Application Firewall (WAF)

(D) IDS

85. Which VPN protocol offers the highest level of security?

(A) PPTP

(B) L2TP/IPSec

(C) OpenVPN

(D) SSTP

86. What does LDAP stand for?

(A) Lightweight Data Access Protocol

(B) Local Directory Access Protocol

(C) Lightweight Directory Access Protocol

(D) Logical Data Access Protocol

87. What is a key component of Network Intrusion Detection Systems (NIDS)?

(A) Firewall rules

(B) Signature-based detection

(C) Data encryption

(D) Packet filtering

88. Which tool can be used to analyze intrusion attempts and correlate data from various logs?

(A) SIEM (Security Information and Event Management)

(B) Snort

(C) Wireshark

(D) Burp Suite

89. Which protocol is typically targeted during DNS poisoning attacks?

(A) TCP

(B) HTTP

(C) UDP

(D) DNS

90. In network forensics, what is the purpose of using a 'mirror port' on a switch?

(A) To block unwanted traffic

(B) To capture and forward traffic to a monitoring device

(C) To increase network bandwidth

(D) To secure wireless connections

91. What does the tcpdump command-line tool do?

(A) Conducts vulnerability assessments

(B) Captures and analyzes live network packets

(C) Generates firewall rules

(D) Scans for open ports

92. Which multiplexing technique does GSM use?

(A) FDMA (Frequency Division Multiple Access)

(B) TDMA (Time Division Multiple Access)

(C) CDMA (Code Division Multiple Access)

(D) SDMA (Space Division Multiple Access)

93. In CDMA (Code Division Multiple Access), how is data transmitted?

(A) Using time slots

(B) Using separate frequencies

(C) Using unique codes for each transmission

(D) By splitting the signal into packets

94. What technology does WAP primarily support?

(A) Voice calls

(B) Secure online transactions

(C) Mobile web browsing

(D) SMS services

95. Which is an advantage of CDMA over TDMA?

(A) Easier implementation

(B) Better resistance to interference

(C) Lower power consumption

(D) Higher cost efficiency

96. Which of the following technologies is primarily used in 2G mobile networks?

(A) CDMA

(B) TDMA

(C) OFDMA

(D) FDMA

97. TDMA divides access to the communication channel based on

(A) frequency bands

(B) time slots

(C) user codes

(D) signal strength

98. Which part of the IMEI identifies the device manufacturer and model?

(A) TAC (Type Allocation Code)

(B) Serial Number

(C) Check Digit

(D) Network Code

99. Which feature in Android helps ensure app sandboxing for security?

(A) SELinux

(B) FileVault

(C) NTFS

(D) iCloud

100. Which of the following best describes packet spoofing?

(A) Encrypting network traffic

(B) Manipulating packet headers to disguise the source IP address

(C) Intercepting data packets in transit

(D) Monitoring network traffic for anomalies

101. Which of the following can prevent VoIP call tampering?

(A) Strong password policies

(B) End-to-end encryption of VoIP traffic

(C) Packet sniffing

(D) MAC address filtering

102. Which tool can detect packet spoofing on a network?

(A) Wireshark

(B) Nmap

(C) Metasploit

(D) Aircrack-ng

103. Which wireless security protocol is considered the most secure?

(A) WEP

(B) WPA

(C) WPA2

(D) WPS

104. What is the main improvement of WPA2 over WPA?

(A) Introduction of AES encryption

(B) Use of RC4 cipher

(C) Implementation of MAC address filtering

(D) Support for packet sniffing

105. What type of encryption does WEP (Wired Equivalent Privacy) use?

(A) AES-256

(B) RC4

(C) SHA-256

(D) Blowfish

106. What is the function of the A3 algorithm in GSM networks?

(A) Encrypts voice data

(B) Authenticates the subscriber

(C) Compresses voice data

(D) Manages call routing

107. Which of the following methods is used to crack WEP keys?

(A) Brute-force attack

(B) Dictionary attack

(C) Passive packet sniffing and IV replay attacks

(D) SQL injection

108. What is the major security threat in WLAN networks?

(A) Dynamic IP addressing

(B) Eavesdropping

(C) Strong encryption standards

(D) Use of firewalls

109. Which of the following is a major forensic challenge with iOS devices?

(A) Open-source nature

(B) Compatibility issues

(C) Strong encryption and closed system architecture

(D) Lack of forensic tools

110. Which forensic tool is commonly used for analyzing SQLite databases in mobile forensics?

(A) FTK Imager

(B) DB Browser for SQLite

(C) Autopsy

(D) EnCase

111. What information do geo-tags in mobile devices contain?

(A) Battery status

(B) GPS coordinates and times stamp

(C) Contact information

(D) App permissions

112. What is the purpose of an IPDR (Internet Protocol Details Record) in forensic analysis?

(A) Monitoring hardware status

(B) Tracking internet usage and IP addresses

(C) Recovering deleted contacts

(D) Extracting call logs

113. In iOS forensics, which of the following is stored in the 'plist' files?

(A) Call logs

(B) System configuration and application data

(C) Multimedia files

(D) Deleted messages

114. What is a common challenge while analyzing CDR data?

(A) Encrypted data

(B) Data inconsistency across carriers

(C) Lack of time stamps

(D) No metadata available

115. What is the role of 'geo-fencing' in mobile forensics?

(A) Restricting access to certain apps

(B) Defining virtual boundaries for tracking devices

(C) Encrypting location data

(D) Monitoring Wi-Fi networks

116. Which type of evidence can be recovered from an SQLite database in a mobile device?

(A) Deleted call logs

(B) App data, messages and browser history

(C) Encryption keys

(D) Firmware details

117. In iOS forensics, which method is typically used for logical data extraction?

(A) NAND mirroring

(B) iTunes backup extraction

(C) Chip-off extraction

(D) Cloud extraction

118. In Android forensics, which command is often used for logical extraction?

(A) adb pull

(B) dd

(C) fsck

(D) chmod

119. Which technique is often used for accessing locked Android devices during forensic investigation?

(A) NAND mirroring

(B) Logical extraction through USB

(C) Brute-force attacks

(D) Chip-off extraction

120. Which of the following forensic tools is best for iOS physical extraction?

(A) Elcomsoft iOS Forensic Toolkit

(B) XRY Logical

(C) Oxygen Forensic Cloud Extractor

(D) FTK Imager

121. Which of the following software tools is designed for forensic timeline analysis?

(A) Magnet AXIOM

(B) Autopsy

(C) Sleuth Kit

(D) EnCase

122. Which of the following is an open-source digital forensics platform that focuses on hard disk analysis and file recovery?

(A) Autopsy

(B) EnCase

(C) FTK (Forensic Toolkit)

(D) Magnet AXIOM

123. Which type of e-business model involves direct interaction between businesses and end consumers?

(A) B2B

(B) C2C

(C) B2C

(D) G2B

124. Which protocol is commonly used to secure e-commerce transactions?

(A) SSL/TLS

(B) FTP

(C) HTTP

(D) IMAP

125. Which of the following best defines cyber espionage?

(A) Monitoring social media activity

(B) Unauthorized access to information system for political or military advantage

(C) Sending spam emails to users

(D) Defaming someone online

126. What legal measure can be taken against cyber squatting?

(A) Filing a complaint under the UDRP (Uniform Domain-Name Dispute-Resolution Policy)

(B) Reporting to local authorities

(C) Disabling the website

(D) Sending an email to ICANN

127. In cyber espionage, 'APT' stands for

(A) Advanced Persistent Threat

(B) Automated Penetration Test

(C) Advanced Phishing Technique

(D) Adaptive Protocol Tool

128. Which Section of the IT Act, 2000 deals with hacking and its penalties?

(A) Section 65

(B) Section 66

(C) Section 67

(D) Section 70

129. Which Amendment introduced the concept of 'cyberterrorism' in the IT Act, 2000?

(A) 2005 Amendment

(B) 2008 Amendment

(C) 2010 Amendment

(D) No Amendment including cyberterrorism

130. Which authority oversees the implementation of the IT Act, 2000 in India?

(A) RBI

(B) Ministry of Electronics and Information Technology (MEITY)

(C) NITI Aayog

(D) Supreme Court of India

131. What is the difference between a digital signature and an electronic signature?

(A) Digital signatures use encryption; electronic signatures may not

(B) Digital signatures are hand written; electronic signatures are not

(C) Electronic signatures use cryptography; digital signatures do not

(D) There is no difference

132. What is the significance of Section 69 of the IT Act, 2000?

(A) Regulation of e-commerce

(B) Protection of personal data

(C) Power to intercept, monitor or decrypt information

(D) Handling cyber defamation cases

133. What is the primary function of the Cyber Regulation Appellate Tribunal (CRAT)?

(A) Investigating cybercrimes

(B) Resolving disputes relate to cyber law violations

(C) Issuing digital certificates

(D) Drafting IT policies

134. Which type of key is used by the recipient to verify a digital signature?

(A) Public key

(B) Private key

(C) Secret key

(D) Hash key

135. Which technology ensures the integrity of electronic evidence in forensic investigations?

(A) Data making

(B) Hashing and digital signatures

(C) Compression algorithms

(D) Optical recognition

136. Which Section of the IT Act, 2000 provides legal recognition to electronic records?

(A) Section 65

(B) Section 4

(C) Section 66

(D) Section 72

137. The Cyber Appellate Tribunal was renamed as

(A) Cyber Legal Tribunal

(B) Appellate Tribunal for Cybersecurity

(C) Telecom Disputes Settlement and Appellate Tribunal (TDSAT)

(D) Information Tribunal

138. Under which Section of the IT Act, 2000 was the Cyber Regulation Appellate Tribunal (CRAT) established?

(A) Section 48

(B) Section 67

(C) Section 10

(D) Section 43

139. Which law in India gives legal recognition to digital signatures?

(A) IT Act, 2000

(B) IPC, 1860

(C) Companies Act, 2013

(D) Evidence Act, 1872

140. What is 'framing' in web design?

(A) Embedding content from another website within a frame on your website

(B) Displaying content in a pop-up window

(C) Creating website layouts with borders

(D) Encrypting page content

141. Which of the following best describes 'linking' in web technology?

(A) Copying content from another website

(B) Connecting one webpage to another via hyperlinks

(C) Encrypting URLs for security

(D) Blocking competitor websites

142. What are metatags primarily used for in web development?

(A) Enhancing website security

(B) Describing the content of web pages to search engines

(C) Creating hyperlinks

(D) Encrypting website data

143. Which legal framework applies to cyberstalking in India under IT Act and IPC?

(A) IT Act Section 66A only

(B) IPC Section 354D and IT Act Section 66A

(C) IT Act Section 67C

(D) IPC Section 420

144. Which Section in the Indian Evidence Act provides for the admissibility of information derived from electronic records stored in mobile phones or computers?

(A) Section 17

(B) Section 3

(C) Section 65B

(D) Section 67

145. Under which Section is the IT Act, 2000 hacking defined and penalized?

(A) Section 43

(B) Section 66

(C) Section 67

(D) Section 72

146. Under which provision can a person be punished for introducing a worm or malware into a computer system?

(A) Section 43(b)

(B) Section 66B

(C) Section 66C

(D) Section 43f

147. What is a common method to bypass a locked Android device during a forensic investigation?

(A) Use of biometric data

(B) Brute-force attack

(C) ADB (Android Debug Bridge) exploits

(D) Over-the-air updates

148. How many digits are there in a standard IMEI number?

(A) 10

(B) 12

(C) 14

(D) 15

149. Which of the following scenarios best illustrates a violation of Section 66G?

(A) Hacking into a Government website

(B) Sending mass spam emails

(C) Using someone else's credit card information without consent

(D) Developing malware

150. In case of a cybersecurity incident, under Section 80, which of the following is true about the role of law enforcement agencies?

(A) They can only investigate cases involving data theft

(B) They are required to report the incident to the National Cyber Security Coordinator

(C) They have the power to take appropriate actions to investigate and take necessary legal action

(D) They cannot act unless a formal complaint is filled

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK

★ ★ ★